

James E. Cecchi
Lindsey H. Taylor
**CARELLA, BYRNE, CECCHI,
OLSTEIN, BRODY & AGNELLO, P.C.**
5 Becker Farm Road
Roseland, NJ 07068
(973) 994-1700

Stuart A. Davidson
Alexander C. Cohen
**ROBBINS GELLER RUDMAN
& DOWD LLP**
225 NE Mizner Boulevard, Suite 720
Boca Raton, FL 33432
(561) 750-3000

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

IN RE: AMERICAN FINANCIAL
RESOURCES, INC. DATA BREACH
LITIGATION

Civil Action No. 22-1757 (MCA) (JSA)

**FIRST AMENDED CONSOLIDATED
CLASS ACTION COMPLAINT and
DEMAND FOR JURY TRIAL**

Plaintiffs Dora Micah (“Micah”), Sharon Styles (“Styles”), Matthew Stuart (“Stuart”), and Anthony A. Oliva, PhD (“Dr. Oliva”) (collectively, “Plaintiffs”), individually and on behalf of all those similarly situated (“Class” or “Class Members”), upon personal knowledge of the facts pertaining to themselves, upon information and belief as to all others, and upon the investigation conducted by their counsel, bring this First Amended Consolidated Class Action Complaint (“Amended Complaint”) against Defendant American Financial Resources, Inc. (“AFR” or “Defendant”) to obtain damages, restitution, and injunctive relief, and in support thereof, state as follows:

NATURE OF THE ACTION

1. This action arises from AFR's failure to properly secure, safeguard, and adequately destroy the sensitive personal identifiable information that was entrusted to it by Plaintiffs and Class Members during the course of its business operations. The types of information at issue include, but is not limited to: Plaintiffs' and Class Members' names, Social Security numbers, driver's license or state-issued identification numbers, and financial account numbers (collectively, "Sensitive Information" or "PII").

2. AFR is a mortgage lending company that provides real estate lending services to thousands of mortgage brokers, bankers, lenders, homeowners, home buyers, realtors, and contractors across the country.

3. Plaintiffs and Class Members include current and former loan customers of AFR; current and former loan customers of an AFR-affiliated institution that shared Plaintiffs' and Class Members' PII with AFR during the course of providing lending or real estate services; and current and former employees of AFR.

4. As part of its services, AFR requires that its customers, including Plaintiffs and Class Members, provide AFR with their PII, including, but not limited to, names, Social Security numbers, and driver's license information.

5. As part of the terms of employment, AFR requires that its employees, including at least Plaintiff Styles and Class Members who are current or past employees of AFR, provide AFR with their PII, including, but not limited to, names, Social Security numbers, and driver's license information.

6. As a lending institution that maintains Plaintiffs' and Class Members' PII, Defendant owed Plaintiffs and Class Members numerous statutory, regulatory, contractual, and

common law duties and obligations, including, but not limited to, those based on its promises to keep Plaintiffs' and Class Members' PII confidential, safe, secure, and protected from unauthorized disclosure, access, dissemination, or theft.

7. Indeed, during the course of its business operations, Defendant expressly and impliedly promised to safeguard Plaintiffs' and Class Members' PII.

8. Furthermore, by obtaining, collecting, using, retaining, and deriving benefit from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties to Plaintiffs and Class Members and knew or should have known that it was responsible for safeguarding and protecting Plaintiffs' and Class Members' PII from unauthorized disclosure access, dissemination, or theft.

9. Plaintiffs and Class Members provided their PII to AFR with the reasonable expectation of privacy and mutual understanding that AFR would comply with its legal duties, obligations, and representations to keep such information confidential, safe, and secure.

10. Plaintiffs and Class Members further reasonably expected and relied upon Defendant to only use their PII for business purposes, implement reasonable retention and data destruction policies, and to make only authorized disclosures of this information.

11. Plaintiffs and Class Members would not have paid the amounts of money they paid for Defendant's services, or surrendered their PII, had they known their information would be maintained using inadequate data security and retention systems.

12. AFR's data security obligations were particularly important given the substantial increase in data breaches preceding the date of this Data Breach, as defined herein.

13. Defendant, however, breached its duties and obligations, and Defendant's failures to honor its obligations increased the risk that Plaintiffs' and Class Members' Sensitive Information would be compromised in the event of a likely cyberattack.

14. Indeed, Defendant's systems did suffer such a fate, and a criminal cyber-attack successfully targeted and accessed Defendant's systems and files that contained Plaintiffs' and Class Members' PII. Upon information and belief, as a result, Plaintiffs' and Class Members' PII was exfiltrated, stolen, disseminated on the Dark Web, and misused to commit identity theft crimes, including as to several Plaintiffs.

15. Beginning on or about March 9, 2022, AFR notified state Attorneys General and/or many of its loan customers about a widespread data breach involving the sensitive PII of thousands of individual loan customers ("Notice Letter").¹ As an example, AFR notified the New Hampshire Attorney General on March 11, 2022 that there were 954 New Hampshire residents affected by the breach.² AFR similarly notified the Washington Attorney General on March 11, 2022 that there were 6,570 Washington residents impacted by the breach, including current or former employees of AFR.³ Following a forensic investigation, which concluded on February 4, 2022, AFR explained through its Notice Letter that, between December 6, 2021 and December 20, 2021,

¹ **Ex. 1**, March 9, 2022 letter from William S. Packer, AFR's Executive Vice President and Chief Operations Officer to Matthew Stuart ("March 9, 2022 Letter").

² Letter from Joseph L. Bruemmer, Baker Hostetler, to Attorney General John Formella, Office of the Attorney General of New Hampshire (Mar. 11, 2022), <https://www.doj.nh.gov/consumer/security-breaches/documents/american-financial-resources-20220311.pdf>.

³ Letter from Joseph L. Bruemmer, Baker Hostetler, to the Office of the Washington Attorney General (Mar. 11, 2022), <https://agportal-s3bucket.s3.amazonaws.com/databreach/BreachM13162.pdf>.

AFR allowed its network to be “accessed without authorization” by unknown third parties, exposing and allowing access to, and acquisition of, the PII for individual customers as detailed above (“Data Breach”).⁴

16. Presaging the harm that Defendant knew would befall victims of its Data Breach, the Notice Letter also advised Plaintiffs and Class Members “to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity.”

17. Notably, while the Data Breach occurred from December 6, 2021 through December 20, 2021, AFR purportedly did not determine what information was accessed until February 4, 2022. Compounding the risk to Plaintiffs and Class Members, AFR then failed to promptly notify the impacted individuals – ultimately, sending the Data Breach notifications over one month later, an unreasonable amount of time from any objective measure.

18. Currently, the full extent of the types of Sensitive Information, the scope of the breach, and the root cause of the Data Breach are all within the exclusive control of Defendant and its agents, counsel, and forensic security vendors at this phase of litigation.

19. Upon information and belief, Defendant is responsible for allowing this Data Breach because of multiple acts of negligence, including, but not limited to: (a) its failure to design, implement, and maintain reasonable data security systems and safeguards; and/or (b) failure to exercise reasonable care in the hiring, supervision, training, and monitoring of its employees and agents and vendors; and/or (c) failure to comply with industry-standard data security practices; and/or (d) failure to comply with federal and state laws and regulations that govern data security and privacy practices and are intended to protect the type of Sensitive Information at issue in this

⁴ March 9, 2022 Letter.

action; and/or (e) failure to design, implement, and execute reasonable data retention and destruction policies.

20. Upon information and belief, despite its role in managing so much Sensitive Information, Defendant failed to take basic security measures such as adequately encrypting its data or following industry security standards to destroy PII that was no longer necessary for the intended business purpose. Moreover, Defendant failed to recognize and detect that unauthorized third parties had accessed its network in a timely manner to mitigate the harm. Defendant further failed to recognize that substantial amounts of data had been compromised, and more likely than not, had been exfiltrated and stolen. Had Defendant not committed the acts of negligence described herein, it would have discovered the Data Breach sooner – and/or prevented the invasion and theft altogether.

21. In this era of frequent data security attacks and data breaches, particularly in the financial industry, Defendant's failures leading to the Data Breach are particularly egregious, as this Data Breach was highly foreseeable.

22. Upon information and belief, based on the type of sophisticated and malicious criminal activity, the type of PII targeted, Defendant's admission that the PII was accessed, Defendants' admission that Plaintiffs' and Class Members' PII was in the files that were accessed, reports of criminal misuse of Plaintiffs' and Class Members' data, and reports of PII on the Dark Web following the Data Breach, Plaintiffs' and Class Members' PII was likely accessed, disclosed, exfiltrated, stolen, disseminated, and used by a criminal third party.

23. To be sure, once Defendant finally realized its computer systems were breached, it was determined that the cybercriminals had continuing, unfettered access to Defendant's network for a full two weeks – from December 6, 2022 through December 20, 2022 – during which they,

among other things, obtained passwords to the network and accessed and downloaded Plaintiffs' and Class Members' PII.

24. As a result of the Data Breach, Plaintiffs and Class Members are at an imminent risk of identity theft.

25. The risk of identity theft is not speculative or hypothetical but is impending and has materialized as there is evidence that Plaintiffs' and Class Members' PII was targeted, accessed, and has been disseminated on the Dark Web. Moreover, Class Members have suffered actual identity theft and misuse of their data following the Data Breach.

26. As Defendant instructed, advised, and warned in its Notice Letters, Plaintiffs and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiffs' and Class Members' have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included, and will include into the future: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against and mitigating against the imminent risk of identity theft.

27. Plaintiffs and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) loss of time heeding Defendant's warnings and following its instructions in the Notice Letter; (f) the loss of benefit of the bargain (price premium damages), to the extent Class Members paid AFR for services; (g) deprivation of value of their PII; and (h) the continued risk to their Sensitive

Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Sensitive Information.

28. Plaintiffs seek to remedy these harms, and to prevent the future occurrence of an additional data breach, on behalf of themselves and all similarly situated persons whose PII was compromised as a result of the Data Breach. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement for loss of time, reimbursement of opportunity costs, out-of-pocket costs, price premium damages, restitution, and injunctive relief including improvements to Defendant's data security systems and protocols, future annual audits, and adequate credit monitoring services funded by the Defendant.

29. Plaintiffs bring this Amended Complaint against Defendant seeking redress for its unlawful conduct, asserting claims for: (a) negligence; (b) negligence *per se*; (c) breach of implied contract; (d) unjust enrichment; (e) violations of New Jersey's state consumer protection statute; and (f) violations of Maryland's and Illinois' state consumer protection statutes.

PARTIES

30. Plaintiff Dora Micah is a citizen of the state of Maryland and resides in Frederick, Maryland. Plaintiff Micah is a consumer who was a customer of Defendant and provided her personal information and PII to Defendant. Defendant notified Plaintiff Micah of the Data Breach and the unauthorized access of her PII by sending her a Notice of Data Breach letter, dated March 9, 2022.

31. Plaintiff Sharon Styles is a citizen of the state of Pennsylvania and resides in Philadelphia, Pennsylvania. Plaintiff Styles was employed by the Defendant and provided her personal information and PII to Defendant in connection with her employment. Defendant notified

Plaintiff Styles of the Data Breach and the unauthorized access of her PII by sending her a Notice of Data Breach letter, dated March 9, 2022, which she did not receive until April 4, 2022.

32. Plaintiff Matthew Stuart is a resident and citizen of Illinois residing in Cook County, Illinois. Plaintiff Stuart is a consumer who was a customer of Defendant and provided his personal information and PII to Defendant. Plaintiff Stuart received AFR's Notice of Data Breach letter, dated March 9, 2022, shortly after that date.

33. Plaintiff Anthony A. Oliva, PhD, is a citizen of the state of Florida and resides in West Miami, Florida. Dr. Oliva is a consumer who was a customer of Defendant and provided his personal information and PII to Defendant. Dr. Oliva received AFR's Notice of Data Breach letter, dated March 9, 2022, shortly after that date.

34. Defendant American Financial Resources, Inc. is a New Jersey corporation, and maintains its principal place of business at 9 Sylvan Way, Parsippany, New Jersey 07054.

35. All of Plaintiffs' claims stated herein are asserted against AFR and any of its owners, predecessors, successors, subsidiaries, agents, and/or assigns.

JURISDICTION AND VENUE

36. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of \$5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one other Class Member (including, for example, named Plaintiff Stuart, a citizen of Illinois) is a citizen of a state different from Defendant (a citizen of New Jersey) to establish minimal diversity.

37. The District of New Jersey has personal jurisdiction over Defendant named in this action because Defendant is incorporated and has its principal place of business in this District;

conducts substantial business in this District through its headquarters, offices, and affiliates; engaged in the conduct at issue here in this District; and otherwise has substantial contacts with this District and purposely availed themselves to the courts in this District.

DEFENDANT’S BUSINESS AND PROMISES

38. AFR operates its business nationwide offering residential financing services to mortgage brokers, bankers, lenders, homeowners, home buyers, realtors, and contractors.

39. In doing so, AFR holds itself out as a full-service mortgage lender, working in wholesale, correspondent, and consumer direct channels. AFR offers a variety of financial options, including FHA, VA, USDA, Ginnie Mae, Fannie Mae, and Freddie Mac. In addition, AFR is a top lender in 203(k) lending for sponsored originations and is one of the nation’s leading renovation and manufactured home lenders. In providing these services, AFR offers an extensive program suite, and “cutting-edge technology.”

40. AFR further holds itself out to be “a group of trusted, innovative, and responsive mortgage professionals who . . . bring a dedicated focus to simplify the lending process.”

41. In the course and scope of its residential financing business, AFR collects massive amounts of highly sensitive PII, including, but not limited to, Social Security numbers, employment information (including tax returns, W-2’s, pay stubs, and letters regarding employment history), credit histories and letters regarding credit events, investment information, addresses, dates of birth, and driver’s license information.

42. AFR has acknowledged the sensitive and confidential nature of the PII. To be sure, collecting, maintaining, and protecting PII is vital to many of AFR’s business purposes.

43. AFR acquired Plaintiffs’ and Class Members’ PII as part of its residential mortgage financing business, and AFR collected and stored the PII for commercial gain.

44. As a condition of their using the services of AFR, consumers were obligated to provide AFR with certain PII, including their name, date of birth, address, Social Security number, driver's license or state-issued identification numbers, telephone number, email address, financial account numbers, and payment card numbers.

45. Plaintiffs and Class Members entrusted their PII to AFR, or an AFR affiliate, on the premise and with the understanding that AFR would safeguard their information, use their PII for business purposes only, not disclose their PII to unauthorized third parties, and/or only retain PII for necessary business purposes and for a reasonable amount of time.

46. AFR has acknowledged the sensitive and confidential nature of the PII. To be sure, collecting, maintaining, retaining, and protecting PII is vital to many of AFR's business purposes. Furthermore, AFR has acknowledged through conduct and statements the PII should only be used for a "legitimate business purpose," that the misuse or inadvertent access, disclosure or unauthorized dissemination of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure.

47. For example, with respect to Social Security numbers, AFR states in its Privacy Policy that:

Social Security numbers are classified as "Confidential" information under the AFR Information Security Policy. As such, Social Security numbers may only be accessed by and disclosed to AFR employees and others with a legitimate business "need to know" in accordance with applicable laws and regulations. Social Security numbers, whether in paper or electronic form, are subject to physical, electronic, and procedural safeguards, and must be stored, transmitted, and disposed of in accordance with the provisions of the Information Security Policy applicable to Confidential information. These restrictions apply to all Social Security numbers

collected or retained by AFR in connection with customer, employee, or other relationships.⁵

48. With respect to privacy in general, AFR states that it is “committed to your financial well-being and protecting the privacy and security of the information you share with us since our inception in 1997.”⁶

49. AFR also makes public representations on its website regarding what information it shares:⁷

We may share information with service providers with whom we work, such as data processors and companies that help us market products and services to you. When permitted, or required by law, we may share information with additional third parties for purposes including response to legal process.

When you submit a loan application to us, we may ask for information that may include where you work, what you do, your income, assets, debts and obligations, your financial goals and other similar information. We use this information when evaluating your eligibility for a loan. This evaluation also requires us to obtain information about you from others such as consumer reporting agencies (also known as credit bureaus), the IRS, licensed title search companies, and your hazard and/or flood insurance company.

In addition, American Financial Resources, Inc. may provide third party firms with information furnished by you, such as names, addresses and the financial information you have provided to us or that we have obtained from others about you. Any use of this information will be restricted to advancing your request for a loan, locating a home, or the marketing of other financial products American Financial Resources, Inc. may offer. We will never sell information about you to any other organization.

We may also provide certain information to others when legally required to do so (for instance, in response to a subpoena), to prevent fraud, or to comply with a request by a government agency or regulator.

⁵ AFR, Privacy Statement (Feb. 1, 2021), <https://www.afrcorp.com/privacy-statement/>.

⁶ *Id.*

⁷ *Id.*

50. Plaintiffs and Class Members, as current and former AFR customers, current and former customers of an AFR affiliate, or AFR employees, were entitled to assume that AFR would uphold its contractual obligations to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, to implement reasonable retention policies, to limit access to authorized individuals, and to make only authorized disclosures of this information.

THE DATA BREACH AND DEFENDANT’S RESPONSE

51. Beginning on or about March 9, 2022, AFR notified many of its customers, current and former employees, and state Attorneys General about a widespread data breach involving sensitive PII of certain current and former customers.

52. Through an investigation, AFR determined that a third-party criminal or criminals accessed its systems between December 6, 2021 and December 20, 2021 (*i.e.*, unauthorized access over 14 calendar days).⁸ The investigation further determined that Plaintiffs’ and thousands of Class Members’ PII were present within the files that were accessed.

53. Thus, for two weeks, unauthorized third parties had access to AFR’s trove of highly sensitive and PII without detection.

54. Upon information and belief, the PII was not encrypted or was not adequately encrypted prior to the Data Breach.

55. The confidential information that was accessed without authorization included names along with data elements including Social Security numbers, account numbers, “and for some individuals, driver’s license number[s].”⁹

⁸ March 9, 2022 Letter.

⁹ *Id.*

56. In response to the Data Breach, AFR waited for over a month after the discovery of the Data Breach, on March 9, 2022 to issue notice. Even then, AFR did not fully disclose the scope of the Data Breach, but opted to issue a vague letter leaving Plaintiffs and Class Members without a full understanding of how the breach occurred or what happened to their PII once it was accessed. For example, the letter fails to mention or provide any conclusive determination as to whether or not the information was exfiltrated, stolen, or taken during the Data Breach, a fact that Plaintiffs and Class Members are entitled to know.

57. In fact, there is no indication by AFR that the investigation concluded that Plaintiffs' and Class Members' PII was safe or that the Data Breach was limited to a mere viewing of the PII, as opposed to theft or exfiltration. To the contrary, the Notice Letter left a strong inference that the PII was not only fully accessed but that the data was likely exfiltrated and disseminated in the attack.

58. Indeed, it is undisputed that the cyber criminals who hacked into Defendant's network accessed and downloaded files stored on Defendant's computer systems.

59. Regardless, Emsisoft, an award-winning malware-protection software company, states that "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence, especially during the preliminary stages of an investigation."¹⁰

60. Consistent with Emsisoft, AFR issued an express warning and advised the impacted individuals of the seriousness of the attack, and that they should "remain vigilant." The Notice

¹⁰ Emsisoft Malware Lab, The chance of data being stolen in a ransomware attack is greater than one in ten (EMSIKFT BLOG July 13, 2020), <https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/>.

Letter further issued specific instructions and mitigation techniques such as “reviewing account statements” for “unauthorized activity” – AFR specifically stated:

We wanted to notify you of the incident and assure you that we take it very seriously. We also encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. If you see charges or activity you did not authorize, please contact your financial institutions immediately.

61. These warnings and instructions were an acknowledgment by AFR that it was not only plausible that the criminals acquired the PII for criminal purposes, thereby placing the impacted customers at an imminent threat of identity theft and financial fraud – but that the theft and dissemination and misuse of the PII is the highly probable result of this type of cyberattack. Indeed, it is undeniable that Plaintiffs’ and Class Members’ PII was accessed and downloaded by the criminals.

62. Without the likelihood of dissemination and misuse, and materialization of identity theft, the warnings and instructions to mitigate the risk would be unnecessary and would cause more harm than good, and Defendant would not have advised such actions that would cost Plaintiffs and Class Members time and money.

63. As an additional line of protection, AFR created and paid for a program that offered identity theft protection to Class Members. Absent an actual, materialized, and imminent threat to the Plaintiffs and Class Members, such a program would also have been unnecessary and a waste of Defendant’s time and money. Defendant would not have spent resources creating such a program without the likelihood that Class Member PII was exfiltrated and disseminated in the attack, and that a materialized and imminent risk of identity theft was present for all Class Members. AFR stated:

Additionally, AFR is offering you a complimentary one-year membership to Kroll’s identity monitoring services. This service helps detect possible misuse of

your personal information and provides you with identity monitoring services focused on immediate identification and resolution of identity theft. . . .¹¹

64. Finally, AFR also acknowledged implementing improvements to its systems stating, “we have implemented additional measures to enhance our security protocols.” These measures included deploying a new advanced endpoint detection and response tool, resetting user passwords, upgrading server and domain controller software, and enhancing multifactor authentication.¹²

65. While AFR admits that enhanced “security protocols” were required to improve its data security systems, there is no indication based solely on the Notice Letter whether these steps are fully adequate to protect Plaintiffs’ and Class Members’ PII going forward, as the source and root cause of the Data Breach were not disclosed and remain unknown and undiscoverable absent litigation.¹³

66. What is evident and indisputable is that the Data Breach resulted in the unauthorized access of Defendant’s systems and files, and that those compromised files contained Plaintiffs’ and thousands of Class Members’ PII (AFR consumers and employees), including their names, Social Security numbers, and driver’s license numbers.

67. Upon information and belief, the cyberattack was targeted at AFR and Plaintiffs’ and Class Members’ PII due to AFR’s status as a major real estate mortgage lending company that collects valuable personal and financial data on its many customers, as well as its employees.

¹¹ March 11, 2022 letter to the Attorney General of New Hampshire, *supra* n.2.

¹² *Id.*

¹³ *Id.*

68. Upon information and belief, the cyberattack was expressly designed to gain access to and steal the private and confidential data, including (among other things) Plaintiffs' and Class Members' PII.

69. Upon information and belief, criminal hackers exfiltrated, stole, disseminated, and have misused Plaintiffs' and Class Members' PII because of the value in exploiting and stealing the identities of Plaintiffs and Class Members.

70. As a result of the Data Breach, the risk of identity theft has materialized, and Plaintiffs and Class Members are at an imminent risk of identity theft.

THE DATA BREACH WAS FORESEEABLE

71. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the financial industry and other industries holding significant amounts of PII preceding the date of the breach.

72. In 2021 alone, there were over 200 data breach incidents.¹⁴ These approximately 200 data breach incidents have impacted nearly 15 million individuals.¹⁵

73. In light of recent high profile data breaches at other industry leading companies, including, Microsoft Corporation (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook, Inc., n/k/a Meta Platforms, Inc. (267 million users, April 2020), The Estee Lauder Companies Inc. (440 million records, January 2020), Whisper (900 million

¹⁴ See Kim Delmonico, *Another (!) Orthopedic Practice Reports Data Breach*, Orthopedics This Week (May 24, 2021), <https://ryortho.com/breaking/another-orthopedic-practice-reports-data-breach/>.

¹⁵ *Id.*

records, March 2020), and Advanced Info Service Public Company Limited (8.3 billion records, May 2020), AFR knew or should have known that its systems would be targeted by cybercriminals.

74. Indeed, cyberattacks against the financial industry have been common for over ten years with the Federal Bureau of Investigation (“FBI”) warning as early as 2011 that cybercriminals were “advancing their abilities to attack a system remotely” and “[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII.” The FBI further warned that that “the increasing sophistication of cyber criminals will no doubt lead to an escalation in cyber crime.”¹⁶

75. Moreover, it is well known that the specific PII at issue in this case, including Social Security numbers and financial account information in particular, is a valuable commodity and a frequent target of hackers.

76. As a sophisticated financial and lending entity that collects, utilizes, and stores particularly sensitive PII, AFR was at all times fully aware of the increasing risks of cyber-attacks targeting the PII it controlled, and its obligation to protect Plaintiffs’ and Class Members’ PII.

77. AFR has acknowledged through conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure.

DEFENDANT FAILED TO PROTECT PLAINTIFFS’ AND CLASS MEMBERS’ PRIVATE INFORMATION

78. Despite the prevalence of public announcements of data breach and data security compromises, and despite Defendant’s own acknowledgment of its duties to keep PII private and

¹⁶ Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), <https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector>.

secure, AFR failed to take appropriate steps to protect Plaintiffs' and Class' PII from being compromised.

79. Defendant did not use reasonable security procedures and practices appropriate to the nature of the Sensitive Information it was maintaining for Plaintiffs and Class Members, causing the exposure of PII of over 200,000 individuals.

A. Defendant Failed to Properly Comply with Federal Trade Commission Data Security Standards

80. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

81. The FTC has brought well publicized enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an "unfair" act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. This includes the FTC's enforcement action against Equifax following a massive data breach involving the personal and financial information of 147 million Americans.

82. In 2016, the FTC updated its publication, "Protecting Personal Information: A Guide for Business," which established cyber-security guidelines for businesses. There, the FTC advised that businesses should protect the PII that they keep by following some minimum standards related to data security, including, among others:

- (a) encrypting information stored on computer networks;
- (b) identifying network vulnerabilities;

- (c) implementing policies to update and correct any security problems;
- (d) utilizing an intrusion detection systems;
- (e) monitoring all incoming traffic for suspicious activity indicating someone is attempting to hack the system;
- (f) watching for large amounts of data being transmitted from the system;
- (g) developing a response plan ready in the event of a breach;
- (h) limiting employee and vendor access to sensitive data;
- (i) requiring complex passwords to be used on networks;
- (j) utilizing industry-tested methods for security;
- (k) verifying that third-party service providers have implemented reasonable security measures;
- (l) educating and training employees on data security practices;
- (m) implementing multi-layer security including firewalls, anti-virus, and anti-malware software; and
- (n) implementing multi-factor authentication.

83. In particular, the FTC further also advised that companies not maintain PII longer than is needed for authorization of a transaction: “If you don’t have a legitimate business need for sensitive personally identifying information, don’t keep it.”¹⁷

84. Upon information and belief, AFR failed to implement or adequately implement at least one of these fundamental data security practices.

¹⁷ FTC, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

85. AFR could have prevented this Data Breach by properly following FTC guidelines by adequately encrypting or otherwise protecting their equipment and computer files containing PII.

86. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

B. Defendant Failed to Comply with Industry Standards

87. The financial industry also routinely incorporates these cybersecurity practices that are standard in AFR's industry. These minimum standards include, but are not limited to:

- (a) maintaining a secure firewall configuration;
- (b) maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;
- (c) monitoring for suspicious or irregular traffic to servers;
- (d) monitoring for suspicious credentials used to access servers;
- (e) monitoring for suspicious or irregular activity by known users;
- (f) monitoring for suspicious or unknown users;
- (g) monitoring for suspicious or irregular server requests;
- (h) monitoring for server requests for PII;
- (i) monitoring for server requests from virtual private networks; and
- (j) monitoring for server requests from Tor exit nodes.

88. Upon information and belief, AFR failed to comply with at least one of these minimal industry standards, thereby opening the door to and causing the Data Breach.

89. AFR could have prevented this Data Breach by properly following industry data security standards by adequately encrypting or otherwise protecting their equipment and computer files containing PII.

90. AFR could also have prevented the scale of the Data Breach simply by designing and implementing data retention practices to delete PII that is no longer needed for an ongoing business purpose.

91. AFR had the resources necessary, and reasonable data security alternatives were known and available to AFR that would have prevented the Data Breach, but AFR neglected to adequately evaluate its systems and invest in adequate security measures, despite its obligation to protect its systems and Plaintiffs' and Class Members' PII.

C. Defendant Failed to Comply with the Gramm-Leach-Bliley Act

92. Defendant is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and, thus, is subject to the GLBA.

93. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [the Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

94. Defendant collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n), and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Defendant was subject to the requirements of the GLBA, 15 U.S.C. § 6801.1, *et seq.*, and is subject to numerous rules and regulations promulgated on the GLBA Statutes. The GLBA Privacy of Consumer Financial Information ("Privacy Rule") became effective on July 1, 2001. *See* 16 C.F.R. § 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the Consumer Financial Protection Bureau ("CFPB") became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that

established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 (“Regulation P”), with the final version becoming effective on October 28, 2014.

95. Accordingly, Defendant’s conduct is governed by the Privacy Rule prior to December 30, 2011, and by Regulation P after that date.

96. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be “clear and conspicuous.” 16 C.F.R. §§ 313.4(a), 313.5(a)(1); 12 C.F.R. §§ 1016.4-1016.5. “Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.” 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must “accurately reflect[] [the financial institution’s] privacy policies and practices.” 16 C.F.R. §§ 313.4(a)(1), 313.5(a)(1); 12 C.F.R. §§ 1016.4-1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution’s security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided “so that each consumer can reasonably be expected to receive actual notice.” 16 C.F.R. § 313.9(a); 12 C.F.R. § 1016.9. As alleged herein, Defendant violated the Privacy Rule and Regulation P.

97. Upon information and belief, Defendant failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers’ PII and storing and/or sharing that PII on its network.

98. Defendant failed to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on its inadequately secured network and would do so after the customer relationship ended.

99. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (a) designating one or more employees to coordinate the information security program; (b) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (c) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (d) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (e) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3-314.4. As alleged herein, Defendant violated the Safeguards Rule.

100. Defendant failed to assess reasonably foreseeable risks to its networks, and to the security, confidentiality, and integrity of PII in its custody or control.

101. Defendant failed to design and implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

102. Defendant failed to adequately oversee service providers.

103. Defendant failed to evaluate and adjust its information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.

THE VALUE OF PII

104. There is both a healthy black market and a legitimate market for the type of PII that was compromised in this action. PII is such a valuable commodity to criminal networks that once the information has been compromised, criminals often trade the information on the “cyber black market” for years.

105. The Sensitive Information of consumers remains of high value to criminals, as evidenced by the prices they will pay through the Dark Web. Numerous sources cite Dark Web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.¹⁸

106. According to the Dark Web Price Index for 2021, payment card details for an account balance up to \$1,000 have an average market value of \$150, credit card details with an account balance up to \$5,000 have an average market value of \$240, stolen online banking logins with a minimum of \$100 on the account have an average market value of \$40, and stolen online

¹⁸ Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends (Oct. 16, 2019), <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/>.

banking logins with a minimum of \$2,000 on the account have an average market value of \$120.¹⁹ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.²⁰

107. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The U.S. Social Security Administration (“SSA”) stresses that the loss of an individual’s Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when they use the credit cards and don’t pay the bills, it damages your credit. You may not find out that someone is using your number until you’re turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.²¹

108. The SSA has further warned that identity thieves can use an individual’s Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, apply for a job using a false identity, open bank accounts, and apply for other government documents such as driver’s licenses and birth certificates.

¹⁹ Zachary Ignoffo, *Dark Web Price Index 2021*, PRIVACY AFFAIRS (Mar. 8, 2021), <https://www.privacyaffairs.com/dark-web-price-index-2021/>.

²⁰ *In the Dark*, VPNOOverview (2019), <https://vpnooverview.com/privacy/anonymous-browsing/in-the-dark/>.

²¹ SSA, *Identity Theft and Your Social Security Number* (June 2021), <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

109. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

110. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

111. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."²²

112. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, Inc., explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x in price on the black market."²³

113. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of personal information. A driver's license can be

²² Brian Naylor, *Victims Of Social Security Number Theft Find It's Hard To Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft>.

²³ Tim Greene, *Anthem hack: Personal data stolen sells for 10x price of stolen credit card numbers*, Computer World (Feb. 6, 2015), <http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html>.

a critical part of a fraudulent, synthetic identity – which go for about \$1200 on the Dark Web. On its own, a forged license can sell for around \$200.”²⁴

114. According to national credit bureau Experian:

A driver’s license is an identity thief’s paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver’s license number, it is also concerning because it’s connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver’s license on file), doctor’s office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you.

Next to your Social Security number, your driver’s license number is one of the most important pieces of information to keep safe from thieves.²⁵

115. According to cybersecurity specialty publication CPO Magazine, “[t]o those unfamiliar with the world of fraud, driver’s license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation.”²⁶ However, this is not the case. As cybersecurity experts point out:

It’s a gold mine for hackers. With a driver’s license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID

²⁴ Lee Matthews, *Hackers Stole Customer’s License Numbers from Geico In Months-Long Breach*, FORBES (Apr. 20, 2021), <https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658>.

²⁵ Sue Poremba, *What Should I Do If My Driver’s License Number is Stolen?* (Oct. 24, 2018), <https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/>.

²⁶ Scott Ikeda, *Geico Data Breach Leaks Driver’s License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, CPO MAGAZINE (Apr. 23, 2021), <https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/>.

verification, or use the information to craft curated social engineering phishing attacks.²⁷

116. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent *The New York Times* article.²⁸

117. In addition, if a Class Member's Social Security number or driver's license number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

**PLAINTIFFS AND CLASS MEMBERS
SUFFERED FORESEEABLE CONCRETE HARMS**

118. As a result of Defendant's ineffective and inadequate data security and retention measures, the Data Breach, and the foreseeable consequences of the PII ending up in the possession of criminals, the risk of identity theft is materialized and imminent.

119. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII, reports of misuse of Class Member PII, and reports of dissemination on the Dark Web, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/Dark Web for sale and purchase by criminals intending to utilize the PII for identity theft crimes, such as opening bank accounts in the victims' names to make purchases or to launder money, filing false tax returns, or filing false unemployment claims.

²⁷ *Id.*

²⁸ Ron Lieber, *How Identity Thieves Took My Wife for a Ride*, N.Y. TIMES (Apr. 27, 2021), <https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html>.

120. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.²⁹ The information disclosed in this Data Breach is impossible to “close” and difficult, if not impossible, to change (such as Social Security numbers).

121. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. The fraudulent activity resulting from the Data Breach may not become evident for years.

122. Indeed, “[t]he risk level is growing for anyone whose information is stolen in a data breach.”³⁰ Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that “[t]he theft of SSNs places consumers at a substantial risk of fraud.”³¹ Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members’ PII will do so at a later date or re-sell it.

123. To date, Defendant has done little to adequately protect Plaintiffs and Class Members, or to compensate them for their injuries sustained in this Data Breach. The

²⁹ See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1>.

³⁰ Susan Ladika, *Study: Data Breaches Pose a Greater Risk*, Fox Business (Mar. 6, 2016), <https://www.foxbusiness.com/features/study-data-breaches-pose-a-greater-risk>.

³¹ THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH-IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, AI PASCAL, JAVELIN STRATEGY & RESEARCH (June 2014), https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf.

complimentary fraud and identity monitoring service offered by Defendant through Experian IdentityWorks is wholly inadequate as the services are only offered for months and it places the burden squarely on Plaintiffs and Class Members by requiring them to expend time signing up for that service, as opposed to Defendant automatically enrolling all victims of this cybercrime.

124. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must, in Defendant's words, "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.

125. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

126. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."³²

127. Plaintiffs' mitigation efforts are also consistent with the steps that the FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: (a) contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity);

³² See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

(b) reviewing their credit reports; (c) contacting companies to remove fraudulent charges from their accounts; (d) placing a credit freeze on their credit; and (e) correcting their credit reports.³³

128. Furthermore, Defendant's poor data security deprived several Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendant or its clients for services, several Plaintiffs and other reasonable consumers understood and expected that they were paying for services and data security, when, in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected.

129. As a result of Defendant's ineffective and inadequate data security and retention measures, the Data Breach, and the imminent risk of identity theft, Plaintiffs and Class Members have suffered numerous actual and concrete injuries, including: (a) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) financial "out of pocket" costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) loss of time due to increased spam and targeted marketing emails; (f) the loss of benefit of the bargain (price premium damages); (g) deprivation of value of their PII; and (h) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Sensitive Information.

PLAINTIFFS' COMMON EXPERIENCES

Plaintiff Micah's Experience

³³ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps> (last visited April 25, 2023).

130. Prior to the Data Breach, AFR received Plaintiff Micah's PII during the course of applying for a mortgage. Upon information and belief, Plaintiff Micah provided her PII to an AFR affiliate who provided her PII to AFR during the course of a mortgage application. Upon information and belief, Plaintiff Micah also paid AFR a fee for its services.

131. Plaintiff Micah is extremely careful about sharing her PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. She stores any and all documents containing PII in a secure location and destroys any documents she receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts. In addition, she password-protects documents containing PII, and does not release her date of birth or other PII on social media sites, etc., as a precautionary measure from identity fraud. Further, she removes all trackers on electronic documents through McAfee which shreds documents to totally remove them online.

132. In March 2022, Plaintiff Micah received a Notice Letter from AFR, substantially similar to **Exhibit 1**, informing her that her full name and Social Security number were accessed by unauthorized third parties, and that her driver's license information was potentially accessed as well. In the Notice Letter, AFR advised her to take certain steps to protect her PII and otherwise mitigate her damages. AFR never notified her that her date of birth was also compromised in the Data Breach.

133. Plaintiff Micah has suffered several varieties of actual injuries as a result of the Data Breach.

134. For example, she has received notifications from McAfee and Experian that her information was found on the Dark Web. Additionally, in June 2022, Plaintiff Micah's husband

experienced at least one unauthorized charge to a payment card linked to account with Plaintiff Micah after the Data Breach. Plaintiff Micah believes this fraudulent charge is directly related to the Data Breach.

135. In addition, Plaintiff Micah has also experienced a substantial increase in suspicious emails and “spam” telephone calls since the Data Breach which she believes were a result of the Data Breach. In fact, she had to cancel the service on her landline telephone service because she was getting an unmanageable amount of robocalls since the Data Breach.

136. Moreover, as a result of the Data Breach and the directives that she received in the Notice Letter, Plaintiff Micah has already spent precious hours dealing with the consequences of the Data Breach (*e.g.*, self-monitoring her bank and credit accounts), as well as her time spent verifying the legitimacy of the Notice of Data Breach letter, communicating with her bank, researching and purchasing multiple forms of security protection services. This time has been lost forever and cannot be recaptured. Moreover, Plaintiff Micah spent this time at Defendant’s direction. Indeed, in the Notice Letter Plaintiff Micah received from Defendant, Defendant directed Plaintiff Micah to spend time mitigating her losses by “reviewing your account statements and credit reports for any unauthorized activity.” Given the short timeframe the attempted identity theft occurred from the time of the Data Breach, it is reasonable to expect that Plaintiff Micah will continue to have to devote significantly more precious time and resources to the aftermath of the Data Breach for many years to come. To date, she (and her husband, with whom she shares joint accounts) have already spent at least 100 hours dealing with the consequences of the Data Breach.

137. On or about April 3, 2022, Plaintiff Micah renewed her McAfee anti-virus protection for \$99.99 for one year as a result of the Data Breach. In addition, she purchased a digital certificate service for her emails which is a security tool that attaches a digital certificate to

her emails verifying that the email has come from her. Plaintiff Micah has paid \$60 for this service. Plaintiff Micah also has enabled enhanced protection on her Verizon accounts to protect intrusions into her cable, internet, and wireless devices.

138. Plaintiff Micah has suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (a) damage to and deprivation in the value of her PII, a form of property that Defendant obtained from the Plaintiff; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

139. Plaintiff Micah also lost the benefit of the bargain and price premium damages for the services she paid for. Had she known that AFR would have inadequate data security practices, she would not have entered into a business transaction, paid for the services, or provided her PII.

140. Plaintiff Micah has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach since she received the Notice Letter. Plaintiff Micah is especially concerned about the theft of her full name paired with her Social Security number and date of birth, which is readily obtainable from the driver's license information which AFR notified Plaintiff Micah may have been stolen in the Data Breach.

141. Plaintiff Micah has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

142. Plaintiff Micah has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in AFR's possession, is protected and safeguarded from future breaches.

Plaintiff Stuart's Experience

143. In or about early 2021, Plaintiff Stuart was a former AFR customer who had used the service on a previous home mortgage. As a condition to receiving the services, AFR required Plaintiff Stuart to supply, and he provided, AFR with his PII, including, but not limited to, his name, address, date of birth, Social Security number, driver's license number, telephone number and email address, to participate in AFR's services. Upon information and belief, at the time of engaging the services, Plaintiff Stuart's PII was entered into AFR systems. Upon information and belief, Plaintiff Stuart paid AFR's a fee for its services.

144. Plaintiff Stuart greatly values his privacy and Sensitive Information, especially when receiving loan and financial services. Plaintiff Stuart has taken reasonable steps to maintain the confidentiality of his PII, and he has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

145. Plaintiff Stuart expected and reasonably relied upon Defendant as part of its services to provide adequate data security to protect the PII that he entrusted to Defendant. If Plaintiff Stuart had known that AFR would not adequately protect his PII, he would not have allowed AFR access to this Sensitive Information, and would not have engaged in business with Defendant.

146. Upon information and belief, Plaintiff Stuart's PII was targeted, accessed, downloaded, and stolen by the third-party criminal actors in the Data Breach. This allegation is supported by the fact that, according to Plaintiffs' cybersecurity expert, Plaintiff Stuart's PII was published for sale on at least four (4) chat groups on the Dark Web following the Data Breach. Indeed, Plaintiff Stuart's PII remains for sale on the Dark Web for up to \$3.00.

147. As a result of the Data Breach and the publication of his PII on the Dark Web, Plaintiff Stuart faces a substantial risk of imminent identity, financial, and health fraud and theft – both now and for years to come. Plaintiff Stuart has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

148. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Stuart faces, Defendant provided Plaintiff Stuart with a one-year subscription to a credit monitoring service. However, Plaintiff Stuart has not sign up for the program, as he already has credit monitoring services from unrelated sources.

149. Moreover, as a result of the Data Breach and the directives that he received in the Notice Letter, substantially similar to **Exhibit 1**, Plaintiff Stuart has already spent precious hours dealing with the consequences of the Data Breach (*e.g.*, self-monitoring his bank and credit accounts, dealing with an attempted home equity line of credit (“HELOC”) fraud), as well as his time spent verifying the legitimacy of the Notice of Data Breach letter, communicating with his bank, and exploring credit monitoring and identity theft insurance options, among other things. This time has been lost forever and cannot be recaptured. Moreover, Plaintiff Stuart spent this time at Defendant’s direction. Indeed, in the Notice Letter Plaintiff Stuart received from Defendant, Defendant directed Plaintiff Stuart to spend time mitigating his losses by “reviewing your account statements and credit reports for any unauthorized activity.” Given the short time-frame the attempted identity theft occurred from the time of the Data Breach, it is reasonable to expect that Plaintiff Stuart will continue to have to devote significantly more precious time and resources to the aftermath of the Data Breach for many years to come.

150. As a result of the Data Breach, Plaintiff Stuart suffered actual injury and damages in paying money to AFR for identity services before the Data Breach; expenditures which he would not have made had AFR disclosed that it lacked data security practices adequate to safeguard PII.

151. Plaintiff Stuart also suffered actual injury in the form of damages and deprivation in the value of his PII – a form of intangible property that he entrusted to AFR for the purpose of providing him services, which was compromised as a result of the Data Breach.

152. Plaintiff Stuart also lost the benefit of the bargain and price premium damages for the services he paid for. Had he known that AFR would have inadequate data security practices, he would not have entered into a business transaction, paid for the services, or provided his PII.

153. Furthermore, Plaintiff Stuart suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has increased concerns for the loss of his privacy, especially his Social Security number.

154. Moving forward, Plaintiff Stuart has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in AFR's possession, and is now protected and safeguarded from future breaches.

Plaintiff Styles' Experience

155. Plaintiff Styles was employed by AFR from August 2014 through August 2017 as a mortgage loan opener. Prior to the Data Breach, AFR received Plaintiff Styles' PII in connection with her employment including her Social Security number and bank account information for the direct deposit of her paychecks from Defendant. Plaintiff Styles has not worked for AFR since August 2017, but AFR continued to possess her PII for almost five years after her employment ended. Thus, AFR had no legitimate business need to keep her PII, much less keep it wholly unsecure.

156. Plaintiff Styles is extremely careful about sharing her PII and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. She does her best to store any and all documents containing sensitive PII in a secure location and destroy any documents she receives in the mail that contain PII or that may contain any information that could otherwise be used to compromise her identity and financial accounts. She shreds all her mail that has her name and address on it. She also diligently chooses unique usernames and passwords for her various online business accounts but does not have any online banking accounts for any of her personal financial accounts. Plaintiff Styles very rarely makes any purchases online but when she has in the past, she did not set up an online account and does not store any credit card information online. In addition, Plaintiff Styles' password-protects documents containing PII, and does not release her date of birth or other PII on social media sites, etc., as a precautionary measure from identity fraud.

157. In April 2022, Plaintiff Styles received the Notice Letter from AFR, substantially similar to **Exhibit 1**, informing her that her full name and Social Security number were accessed by unauthorized third parties, and that her driver's license information was potentially accessed as well. In the Notice Letter, AFR advised Plaintiff Styles to take certain steps to protect her PII and otherwise mitigate her damages. AFR never notified Plaintiff Styles that her date of birth was also compromised in the Data Breach.

158. Plaintiff Styles has suffered several varieties of actual injuries as a result of the Data Breach.

159. Specifically, as a direct and proximate result of the Data Breach, Plaintiff Styles has become a recent victim of identity theft and has had an unauthorized person make numerous attempts to withdraw money from her savings account at Santander Bank, which is the same bank

and account number that she provided to AFR in connection with her employment. The first incident occurred on May 9, 2022, when an unauthorized person representing themselves as Plaintiff Styles, presented a fictitious driver's license to a bank teller at a Santander bank branch in New York City attempting to withdraw \$9,300 from her savings account. The bank teller would not allow the withdrawal and notified Plaintiff Styles. This unauthorized person had set up an online banking account in Plaintiff Styles' name. Plaintiff Styles does not have an online banking account. Later that day, the same incident happened at another Santander branch in New York City where an unauthorized person attempted to withdraw \$8,500 from Plaintiff Styles' account. On May 10, 2022, there was another unauthorized attempt to withdraw money from Plaintiff Styles' account in New York. On May 13, 2022, Plaintiff Styles went to her local Santander branch to close out her compromised bank accounts and opened two new accounts. On May 14, 2022, Plaintiff Styles received a phone call from a teller at a Santander branch in the Bronx informing her that someone representing themselves as Plaintiff Styles, presented a fictitious passport and Plaintiff Styles' new account information to withdraw money from Plaintiff Styles' bank account. Luckily, this unauthorized transaction was denied by the teller. On May 16, 2022, Plaintiff Styles closed her bank accounts at Santander Bank and had to open new accounts at another bank in order to protect her financial accounts.

160. Plaintiff Styles has also experienced numerous unauthorized charges on one of her credit cards following the Data Breach. She had unauthorized charges on her credit card statement from February 23, 2022, from apple.com for \$10.79 and from February 25, 2022, for a Microsoft yearly plan for \$75.59. Plaintiff Styles had to cancel her credit card and was without a credit card for approximately ten days until she received a new card.

161. Plaintiff Styles has also experienced a substantial increase in suspicious emails and “spam” telephone calls since the Data Breach which she believes are a result of the Data Breach. She has blocked over 100 scam phone numbers on her mobile device since the Data Breach.

162. Moreover, as a result of the Data Breach and the directives that she received in the Notice Letter, Plaintiff Styles has already spent precious hours dealing with the consequences of the Data Breach (*e.g.*, self-monitoring her bank and credit accounts), as well as her time spent verifying the legitimacy of the Notice of Data Breach letter, communicating with her bank and making numerous trips to her bank and a new bank to close bank accounts and open new bank accounts, putting a freeze on her credit with Equifax, Experian, and Trans Union and having to unlock these credit freezes to open up new bank accounts and then relock the freezes, exploring credit monitoring and identity theft insurance options, among other things. This time has been lost forever and cannot be recaptured. Moreover, Plaintiff Styles spent this time at Defendant’s direction. Indeed, in the Notice Letter Plaintiff Styles received from Defendant, Defendant directed Plaintiff Styles to spend time mitigating her losses by “reviewing your account statements and credit reports for any unauthorized activity.” Given the short timeframe the attempted identity theft occurred from the time of the Data Breach, it is reasonable to expect that Plaintiff Styles will continue to have to devote significantly more precious time and resources to the aftermath of the Data Breach for many years to come. To date, she has already spent at least 30 hours dealing with the consequences of the Data Breach.

163. Plaintiff Styles has suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (a) damage to and deprivation in the value of her Sensitive Information, a form of property that Defendant obtained from Plaintiff Styles; and

(b) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

164. Plaintiff Styles has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and she has suffered increased concerns for the loss of her privacy since Plaintiff Styles received the Notice Letter. She is especially concerned about the theft of her full name paired with her Social Security number and date of birth, which is readily obtainable from the driver's license information which AFR notified her may have been stolen in the Data Breach.

165. Plaintiff Styles has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

166. Plaintiff Styles has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in AFR's possession, is protected and safeguarded from future breaches.

Plaintiff Oliva's Experience

167. Prior to the Data Breach, AFR received Dr. Oliva's PII after purchasing his mortgage from his prior lender. Thereafter, AFR sold his mortgage to TIAA-CREF (effective December 1, 2018), but continued to possess Dr. Oliva's PII after the sale for more than three years, and the Data Breach occurred more than three years after that mortgage sale. Thus, AFR had no legitimate business need to keep Dr. Oliva's PII, much less keep it wholly unsecured.

168. Dr. Oliva is extremely careful about sharing his PII and has made his best efforts to not knowingly transmit unencrypted PII over the internet or any other unsecured source. He

also does his best to store any and all documents containing sensitive PII in a secure location, and destroys documents he receives in the mail that contain PII or that may contain information that could otherwise be used to compromise his identity and financial accounts, or otherwise secures in a locked filing cabinet or personal safe for documents that need to be retained. He also diligently chooses unique usernames and passwords for his various online accounts. In addition, Dr. Oliva password-protects documents containing PII, and does not release his date of birth on social media sites, etc., as a precautionary measure from identity fraud.

169. To prevent PII compromise and fraudulent activity against his bank and other accounts, Dr. Oliva has intentionally requested from his bank not to have a debit card. Instead, Dr. Oliva only uses third-party credit cards for all purchases as much as possible, including separate credit cards for consumer purchases and utilities, to protect his bank and other accounts. These cards are then paid in full each month. In addition, Dr. Oliva does not have personal identification numbers set up on his credit card as an extra layer of protection to prevent unauthorized cash advance withdrawals.

170. In March 2022, Dr. Oliva received the Notice Letter from AFR, substantially similar to **Exhibit 1**, informing him that his full name and Social Security number were accessed by unauthorized third parties, and that his driver's license information was potentially accessed as well. In the Notice Letter, AFR advised Dr. Oliva to take certain steps to protect his PII and otherwise mitigate his damages. AFR never notified Dr. Oliva that his date of birth was also compromised in the Data Breach.

171. Dr. Oliva has suffered several varieties of actual injuries as a result of the Data Breach.

172. Specifically, as a direct and proximate result of the Data Breach, Dr. Oliva has become a recent victim of identity theft and has had an unauthorized person attempt to fraudulently obtain a HELOC in his name. As a result, Dr. Oliva's credit score dropped, which negatively impacts his ability to receive financing as well as negatively impacts potential interest rates for consumer items.

173. Moreover, as a result of the Data Breach and the directives that he received in the Notice Letter, Dr. Oliva has already spent precious hours dealing with the consequences of the Data Breach (*e.g.*, self-monitoring his bank and credit accounts, dealing with an attempted HELOC fraud), as well as his time spent verifying the legitimacy of the Notice of Data Breach letter, communicating with his bank, exploring credit monitoring and identity theft insurance options, among other things. This time has been lost forever and cannot be recaptured. Moreover, Dr. Oliva spent this time at Defendant's direction. Indeed, in the Notice Letter Dr. Oliva received from Defendant, Defendant directed Dr. Oliva to spend time mitigating his losses by "reviewing your account statements and credit reports for any unauthorized activity." Given the short time-frame the attempted identity theft occurred from the time of the Data Breach, it is reasonable to expect that Dr. Oliva will continue to have to devote significantly more precious time and resources to the aftermath of the Data Breach for many years to come.

174. Furthermore, Dr. Oliva has suffered an injury in the form of deprivation in the value of his PII, which is a form of property, insofar as its value has been diminished by the Data Breach.

175. Dr. Oliva has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and he has suffered increased concerns for the loss of his privacy since he received the Notice Letter. He is especially concerned about the theft of his full name paired

with his Social Security number and date of birth, which is readily obtainable from the driver's license information which AFR notified him may have been stolen in the Data Breach.

176. Dr. Oliva has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

177. Dr. Oliva has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in AFR's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

178. Plaintiffs bring this Amended Complaint on behalf of themselves and Class Members pursuant to Fed. R. Civ. P. 23(b)(2), (b)(3), and (c)(4).

179. Plaintiffs seek to remedy those harms described herein on behalf of themselves and all similarly situated persons whose PII was accessed unlawfully during the Data Breach.

180. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

All persons residing in the United States whose PII was compromised in the Data Breach ("Nationwide Class" or "Class").

181. The Nationwide Class asserts claims under New Jersey law against AFR for: (a) negligence; (b) negligence *per se*; (c) breach of implied contract; (d) unjust enrichment; and (e) violations of the New Jersey Consumer Fraud Act ("New Jersey CFA").

182. Alternatively, Plaintiffs seek certification of Florida, Maryland, Illinois, and Pennsylvania law claims on behalf of alternative Florida, Maryland, Illinois, and Pennsylvania Classes, defined as follows:

All natural persons residing in [Florida, Maryland, Illinois, or Pennsylvania] whose PII was compromised in the Data Breach (“[Florida, Maryland, Illinois, or Pennsylvania] Class”).

183. The alternative Florida, Maryland, Illinois, and Pennsylvania Classes assert claims under their respective state laws against AFR for violations of state consumer protection statutes and/or state common law.

184. Excluded from the Nationwide Class and the alternative Florida, Maryland, Illinois, and Pennsylvania Classes are AFR, any entity in which either AFR has a controlling interest, and either AFR’s officers, directors, legal representatives, successors, subsidiaries, and agents; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and any and all federal, state, or local governments, including, but not limited to, their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions. Also excluded from the Nationwide Class and the alternative Florida, Maryland, Illinois, and Pennsylvania Classes are any judicial officers presiding over this matter, members of their immediate family, and members of their judicial staff.

185. Numerosity, Fed R. Civ. P. 23(a)(1): The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Nationwide Class consists of over 200,000 individuals whose sensitive data was compromised in the Data Breach. The alternative Florida, Maryland, Illinois, and Pennsylvania Classes more than likely contains thousands of Class Members throughout each of the states.

186. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, but are not limited to:

- (a) whether AFR breached a duty to Class Members to safeguard their PII;
- (b) whether AFR expressly or impliedly promised to safeguard Plaintiffs' and Class Members' PII;
- (c) whether AFR unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII;
- (d) whether AFR failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- (e) whether AFR's data security systems prior to, during, and after the Data Breach complied with the applicable FTC data security laws and regulations;
- (f) whether AFR's data security systems prior to and during the Data Breach were consistent with industry standards, as applicable;
- (g) whether unauthorized third parties accessed or obtained Class Members' PII in the Data Breach;
- (h) whether AFR knew or should have known that its data security systems and monitoring processes were deficient;
- (i) whether Plaintiffs and Class Members suffered legally cognizable injuries as a result of the AFR's misconduct;
- (j) whether AFR's conduct was negligent;
- (k) whether AFR breached expressed or implied contractual obligations;
- (l) whether AFR violated the New Jersey CFA;
- (m) whether AFR violated Maryland's or Illinois' state consumer protections statutes;
- (n) whether AFR was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;
- (o) whether AFR adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur; and
- (p) whether Plaintiffs and Class Members are entitled to damages, civil penalties, restitution, and/or injunctive relief.

187. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

188. Adequacy of Representation, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiffs' counsel are competent and experienced in litigating class actions and data breach cases.

189. Predominance, Fed. R. Civ. P. 23(b)(3): AFR has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all of Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from AFR's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

190. Superiority, Fed. R. Civ. P. 23(b)(3): A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would, therefore, have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for AFR. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

191. Manageability, Fed. R. Civ. P. 23(b)(3): The litigation of the claims brought herein is manageable. AFR's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action. Adequate notice can be given to Class Members directly using information maintained in AFR's records.

192. Conduct Generally Applicable to the Class, Fed. R. Civ. P. 23(b)(2): Further, AFR has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive relief with regard to Class Members as a whole is appropriate. Unless a class-wide injunction is issued, AFR may continue in its failure to properly secure Class Members' PII, AFR may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and AFR may continue to act unlawfully as set forth in this Amended Complaint.

193. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. The particular issues include, but are not limited to:

- (a) whether AFR owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
- (b) whether AFR breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
- (c) whether AFR failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- (d) whether an implied contract existed between AFR on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;
- (e) whether AFR breached the implied contract;

- (f) whether AFR failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- (g) whether AFR engaged in unfair or unconscionable practices by failing to safeguard Plaintiffs' and Class Members' PII; and
- (h) whether Class Members are entitled to actual damages, statutory damages, nominal damages, restitution, injunctive relief, and/or punitive damages as a result of AFR's wrongful conduct.

**CLAIMS ON BEHALF OF THE NATIONWIDE CLASS AND ALTERNATIVE
FLORIDA, MARYLAND, ILLINOIS AND PENNSYLVANIA CLASSES**

**COUNT I
NEGLIGENCE**

(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the Florida, Maryland, Illinois, and Pennsylvania Classes)

194. Plaintiffs repeat the allegations contained in paragraphs 1 through 193 as if fully set forth herein.

195. Plaintiffs bring this Count on behalf of themselves and the Nationwide Class or alternatively, the Florida, Maryland, Illinois, and Pennsylvania Classes.

196. AFR owed several common law duties to Plaintiffs and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' PII within its control from being accessed, compromised, exfiltrated, and stolen by criminal third parties in foreseeable cyber-crimes.

197. First, a common law duty arose by the foreseeability of the cyber-crimes. Due to the ongoing threat and highly publicized cyber-attacks businesses like AFR that acquire and store PII, AFR was on notice of the substantial and foreseeable risk of a cyber-attack on its systems, and that Plaintiffs and Class Members would be harmed if AFR did not protect Plaintiffs' and Class Members' Sensitive Information from threat actors.

198. AFR knew or should have known that its systems were vulnerable to unauthorized access and exfiltration by criminal third parties. AFR knew, or should have known, of the importance of safeguarding Plaintiffs' and Class Members' PII – including Social Security numbers, driver's license numbers, and financial account information. AFR further knew or should have known of the foreseeable consequences and harm to Plaintiffs and Class Members, if AFR's data security system and network was breached – including, specifically, the risk of identity theft and related costs imposed on Plaintiffs and Class Members as a result of a data breach. AFR knew or should have known about these risk and dangers to Plaintiffs and Class Members and taken steps to strengthen its data, information technology, and email handling systems accordingly.

199. Second, by obtaining, collecting, using, retaining, and deriving benefits from Plaintiffs' and Class Members' PII, Defendant assumed the legal duty to protect Plaintiffs' and Class Members' PII from foreseeable cyber-crimes.

200. Third, AFR's duty to use reasonable data security measures arose as a result of the special relationship that existed between AFR and the Plaintiffs and Class Members. The special relationship arose because AFR received Plaintiffs' and Class Members' confidential data as part of the financial process for obtaining residential mortgages. AFR was in the sole position to ensure that it had sufficient safeguards to protect against the harm to Plaintiffs and Class Members that would result from a data breach.

201. Finally, AFR's duties arose by statute under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair or deceptive acts or practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal and confidential information. Various FTC publications and data security breach orders further form the basis of AFR's duty.

202. AFR breached its respective common law and statutory duties by failing to provide data security consistent with industry standards to ensure that its systems and networks adequately protected the PII it had been entrusted against foreseeable cyber-crimes. AFR did not use reasonable security procedures and practices appropriate for the nature of the sensitive information it was maintaining, causing Plaintiffs' and Class Members' PII to be exposed. As a result, AFR increased the risk to Plaintiffs and Class Members that their PII would be compromised and stolen in a cyber-crime.

203. Plaintiffs' and Class Members' PII would not have been compromised in the Data Breach but for AFR's wrongful and negligent breach of its duties.

204. Neither Plaintiffs nor, upon information and belief, the other Class Members contributed to the Data Breach or subsequent misuse of their PII as described in this Amended Complaint.

205. AFR breached its obligations to Plaintiffs and Class Members and was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Upon information and belief, AFR could have prevented this Data Breach by encrypting, or adequately encrypting, or otherwise protecting their equipment and computer files containing Plaintiffs' and Class Members' PII.

206. Upon information and belief, AFR's negligent conduct also includes, but is not limited to, one or more of the following acts and omissions:

- (a) failing to maintain and update an adequate data security system to reduce the risk of data breaches;
- (b) failing to adequately train employees to protect consumers' PII;
- (c) failing to adequately monitor, evaluate, and ensure the security of its network and systems;

- (d) failing to properly monitor its own data security systems for existing intrusions;
- (e) failing to comply with the minimum FTC guidelines for cybersecurity, in violation of the FTC Act;
- (f) failing to adhere to industry standards for cybersecurity;
- (g) failing to encrypt or adequately encrypt the PII;
- (h) failing to implement reasonable data retention policies; and
- (i) was otherwise negligent.

207. Furthermore, AFR was plainly aware that it should destroy any PII that it no longer needed to service a mortgage (*e.g.*, where AFR sold its mortgage-servicing on a particular mortgage to another company), or for the purposes of employment, or at least should have ensured extra precautions to secure such PII since, under such circumstances, there was effectively no longer a “legitimate business ‘need to know’” for accessing it.

208. As a direct and proximate result of Defendant’s negligent acts and/or omissions, Plaintiffs’ and Class Members’ PII was compromised, and they are all at a high risk of identity theft and financial fraud for many years to come. Plaintiffs and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the risk of future identity theft; (b) loss of time and loss of productivity incurred mitigating the risk of future identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) deprivation of value of PII; and (f) the continued risk to their Sensitive Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs’ and Class Members’ Sensitive Information.

209. Plaintiffs seek to remedy these harms, and to prevent the future occurrence of an additional data breach, on behalf of themselves and all similarly situated persons whose Sensitive

Information were compromised as a result of the Data Breach. Plaintiffs seek compensatory damages for loss of time, opportunity costs, out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems and protocols, future annual audits, and adequate credit monitoring services funded by the Defendant.

210. Accordingly, Plaintiffs, individually and on behalf of all those similarly situated, seek an order awarding damages in an amount to be determined at trial.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the Florida, Maryland, Illinois, and Pennsylvania Classes)

211. Plaintiffs repeat the allegations contained in paragraphs 1 through 193 as if fully set forth herein.

212. Plaintiffs bring this Count on behalf of themselves and the Nationwide Class or alternatively, the Florida, Maryland, Illinois, and Pennsylvania Classes.

213. The FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as AFR, of failing to use reasonable measures to protect PII. 15 U.S.C. § 45(a)(1).

214. The FTC publications and orders described above also form part of the basis of AFR's duty in this regard.

215. AFR violated the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. AFR's conduct was particularly unreasonable given the nature and amount of PII it obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving companies as large as AFR, including, specifically, the immense damages that would result to Plaintiffs and Class Members.

216. AFR's violations of the FTC Act, as interpreted by the FTC to include a duty to employ adequate and reasonable data security measures, constitute negligence *per se*.

217. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

218. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

219. Similarly, the Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

220. AFR violated the Safeguards Rule by failing to: (a) assess reasonably foreseeable risks to the security, confidentiality, and integrity of PII in its custody or control; (b) design and implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures; (c) adequately oversee service providers; and (d) evaluate and adjust its information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.

221. AFR's violations of the GLBA constitute negligence *per se*.

222. Plaintiffs and Class Members are within the class of persons that the GLBA was intended to protect.

223. The harm that occurred as a result of the Data Breach is the type of harm the GLBA was intended to guard against.

224. As a direct and proximate result of AFR's negligence *per se* under the FTC Act and GLBA, Plaintiffs and the Class have suffered, continue to suffer, and will suffer, injuries, damages, and harm as set forth herein.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the Florida, Maryland, Illinois, and Pennsylvania Classes)

225. Plaintiffs repeat the allegations contained in paragraphs 1 through 193 as if fully set forth herein.

226. Plaintiffs bring this Count on behalf of themselves and the Nationwide Class in the alternative to all other Counts alleged herein.

227. For years and continuing to today, AFR's business model has depended upon it being entrusted with customers' PII. Trust and confidence are critical and central to the services provided by AFR in the residential financing industry. Unbeknownst to Plaintiffs and absent Class Members, however, AFR did not secure, safeguard, or protect its customers' and employees' data and employed deficient security procedures and protocols to prevent unauthorized access to customers' PII. AFR's deficiencies described herein were contrary to their security messaging.

228. Plaintiffs and absent Class Members received services from AFR, and AFR was provided with, and allowed to collect and store, their PII on the mistaken belief that AFR complied with their duties to safeguard and protect its customers' and employees' PII. Upon information and belief, putting their short-term profit ahead of safeguarding PII, and unbeknownst to Plaintiffs and absent Class Members, AFR knowingly sacrificed data security in an attempt to save money.

229. Upon information and belief, AFR knew that the manner in which they maintained and transmitted customer PII violated industry standards and their fundamental duties to Plaintiffs and absent Class Members by neglecting well-accepted security measures to ensure confidential information was not accessible to unauthorized access. AFR had knowledge of methods for designing safeguards against unauthorized access and eliminating the threat of exploit, but it did not use such methods.

230. AFR had within its exclusive knowledge, and never disclosed, that they had failed to safeguard and protect Plaintiffs' and absent Class Members' PII. This information was not available to Plaintiffs, absent Class Members, or the public at large.

231. AFR also knew that Plaintiffs and absent Class Members expected security against known risks and that they were required to adhere to state and federal standards for the protection of confidential personally identifying, financial, and other personal information.

232. Plaintiffs and absent Class Members did not expect that AFR would knowingly insecurely maintain and hold their PII when that data was no longer needed to facilitate a business transaction or other legitimate business reason. Likewise, Plaintiffs and absent Class Members did not know or expect that AFR would employ substantially deficient data security systems and fail to undertake any required monitoring or supervision of the entrusted PII.

233. Had Plaintiffs and absent Class Members known about AFR's efforts to deficiencies and efforts to hide their ineffective and substandard data security systems, Plaintiffs and absent Class Members not have entered into business dealings with AFR.

234. By withholding the facts concerning the defective security and protection of customer PII, AFR put their own interests ahead of the very customers who placed their trust and

confidence in AFR, and benefitted themselves to the detriment of Plaintiffs and absent Class Members.

235. As a result of its conduct as alleged herein, AFR sold more services than it otherwise would have, and was able to charge Plaintiffs and Class Members more for AFR's mortgage services than it otherwise could have. AFR was unjustly enriched by charging for and collecting for those services that it would not have obtained to the detriment of Plaintiffs and absent Class Members.

236. It would be inequitable, unfair, and unjust for AFR to retain these wrongfully obtained fees and benefits. AFR's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

237. AFR's unfair and deceptive conduct to not disclose those defects have, among other things, caused Plaintiffs and Class Members to enter into a business arrangement that was deceptive and dangerous to their identities.

238. As a result, Plaintiffs paid for services that they would not have paid for had Defendant disclosed the inadequacy of its data security practices.

239. Plaintiffs and each member of the proposed Class are each entitled to restitution and non-restitutionary disgorgement in the amount by which AFR were unjustly enriched, to be determined at trial.

COUNT IV
BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, the Florida, Maryland, Illinois, and Pennsylvania Classes)

240. Plaintiffs repeat the allegations contained in paragraphs 1 through 193 as if fully set forth herein.

241. Plaintiffs bring this Count on behalf of themselves and the Nationwide Class or alternatively, the Florida, Maryland, Illinois, and Pennsylvania Classes.

242. When Plaintiffs and Class Members paid money and provided their PII to AFR in exchange for goods or services, they entered into implied contracts with AFR pursuant to which AFR agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

243. AFR solicited and invited prospective customers to provide their PII as part of its regular business practices. As a condition of receiving services or being eligible for employment, Defendant required Plaintiffs and Class Members to provide their PII, including names, Social Security numbers, driver's license numbers, addresses, dates of birth, email addresses, financial account numbers, and payment card numbers.

244. Pursuant to FTC guidelines and standard practice in the financial industry, AFR was obligated to take reasonable steps to maintain the security of Plaintiffs' and Class Members' PII. As a result, by requesting that Plaintiffs and Class Members provide their PII as part of their doing business with AFR, AFR implicitly promised to adhere to these industry standards.

245. Plaintiffs and Class Members each accepted AFR's offers and provided their PII to AFR. In entering into such implied contracts, Plaintiffs and the Class reasonably believed that AFR's data security practices and policies were reasonable and consistent with industry standards, and that AFR would use part of the fees received from Plaintiffs and the Class to pay for adequate and reasonable data security practices to safeguard the PII.

246. Plaintiffs and Class Members accepted Defendant's offers and provided their PII to Defendant. Defendant accepted the PII, and there was a meeting of the minds that Defendant would secure, protect, and keep the PII confidential.

247. Plaintiffs fully performed their obligations under the implied contracts with Defendant.

248. Plaintiffs would not have entered into transactions with AFR if Plaintiffs had known that AFR would not protect their PII.

249. Plaintiffs and the Class would not have provided and entrusted their PII to AFR in the absence of the implied contract between them and AFR to keep the information secure.

250. Plaintiffs and the Class fully performed their obligations under the implied contracts with AFR.

251. AFR breached its implied contracts with Plaintiffs and the Class by failing to safeguard and protect their PII and by failing to provide timely and accurate notice that their PII was compromised as a result of the Data Breach.

252. As a direct and proximate result of AFR's breaches of their implied contracts, Plaintiffs and the Class sustained actual losses and damages as described herein.

COUNT V
NEW JERSEY CONSUMER FRAUD ACT, N.J.S.A. § 56:8-2
(On Behalf of Plaintiffs and the Nationwide Class)

253. Plaintiffs repeat the allegations contained in paragraphs 1 through 193 as if fully set forth herein.

254. Plaintiffs bring this Count on behalf of themselves and the Nationwide Class.

255. The New Jersey CFA makes unlawful "[t]he act, use or employment by any person of any *unconscionable commercial practice*, deception, fraud, false pretense, false promise, misrepresentation, or the knowing concealment, suppression or omission of any material fact with the intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of

such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby.” N.J.S.A. § 56:8-2 (emphasis added).

256. AFR, Plaintiffs, and Class Members are “persons” within the meaning of N.J.S.A. § 56:8-1(d).

257. AFR engaged in “sales” of “merchandise” within the meaning of N.J.S.A. § 56:8-1(c), (d).

258. Plaintiffs and Class Members are consumers who made payments to Defendant for the furnishing of financial services that were primarily for personal, family, or household purposes.

259. New Jersey CFA claims for unconscionable commercial practice need not allege any fraudulent statement, representation, or omission by the defendant. *Dewey v. Volkswagen AG*, 558 F. Supp. 2d 505, 525 (D.N.J. 2008); *see also Cox v. Sears Roebuck & Co.*, 138 N.J. 2, 19 (1994).

260. “The standard of conduct that the term ‘unconscionable’ implies is lack of ‘good faith, honesty in fact and observance of fair dealing.’” *Cox*, 138 N.J. 2 at 18 (quoting *Kugler v. Romain*, 58 N.J. 522, 544 (1971)). “In addition, “[i]ntent is not an essential element” for allegations related to unconscionable commercial practices to succeed.” *Fenwick v. Kay Am. Jeep, Inc.*, 72 N.J. 372, 379 (1977).

261. Here, AFR’s conduct was unconscionable under the New Jersey CFA in its failure to maintain adequate data security and to safeguard their PII.

262. Specifically, AFR’s handling and protection of Plaintiffs’ and Class Members’ PII was an unconscionable commercial practice for the following reasons, among others.

263. Plaintiffs and Class Members had no choice as to whether to provide their PII to AFR nor the categories of PII in order to use AFR’s services.

264. The terms and conditions under which Plaintiffs and Class Members agreed to provide PII to AFR, and how AFR was to protect their PII were non-negotiable and were presented on a take-it-or-leave it basis to Plaintiffs and Class Members.

265. Plaintiffs and Class Members were unable to discover the true state of AFR's data security measures and take measures on their own to protect their PII once it was in AFR's possession. Thus, Plaintiffs and Class Members were completely dependent upon AFR to protect their PII once it was in AFR's possession.

266. Indeed, AFR lulled Plaintiffs and Class Members into a false sense of security by representing that their PII would be well-taken-care-of. AFR specifically states in its Privacy Policy that:

Social Security numbers are classified as “Confidential” information under the AFR Information Security Policy. As such, Social Security numbers may only be accessed by and disclosed to AFR employees and others with a legitimate business “need to know” in accordance with applicable laws and regulations. Social Security numbers, whether in paper or electronic form, are subject to physical, electronic, and procedural safeguards, and must be stored, transmitted, and disposed of in accordance with the provisions of the Information Security Policy applicable to Confidential information. These restrictions apply to all Social Security numbers collected or retained by AFR in connection with customer, employee, or other relationships.³⁴

267. With respect to privacy in general, AFR stated that it is “committed to your financial well-being and protecting the privacy and security of the information you share with us since our inception in 1997.”³⁵

268. AFR's data protection practices were further unconscionable because AFR:

³⁴ AFR, Privacy Statement (Feb. 1, 2021), <https://www.afrcorp.com/privacy-statement/>.

³⁵ *Id.*

- a. continued to store and maintain the PII of former customers when AFR had no legitimate business need to do so;
- b. continued to gather and store PII, and other personal information after AFR knew or should have known of the security vulnerabilities of its computer systems that were exploited in the Data Breach; and
- c. continued to gather and store PII, and other personal information after AFR knew or should have known of the Data Breach and before AFR allegedly remediated the data security incident.

269. AFR's data protection practices are contrary to public policy in that they fail to comply with FTC rules and regulations relating to data security and other applicable standards as is set forth above.

270. AFR still possesses Plaintiffs' and Class Members' PII, and that PII has been both accessed and misused by unauthorized third parties. Plaintiffs and Class Members will have to spend the remainder of their lives at greater risk for identity theft and fraud (having to constantly monitor for the same).

271. The foregoing unconscionable commercial practices emanated from New Jersey and were directed at consumers/purchasers in New Jersey and in each state where Defendant did business.

272. As a direct and proximate result of AFR's multiple, separate violations of N.J.S.A. § 56:8-2, Plaintiffs and Class Members suffered ascertainable losses including, but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in AFR's

possession and is subject to further unauthorized disclosures so long as AFR fails to undertake appropriate and adequate measures to protect the PII in its continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (g) the diminished value of AFR's services they received.

273. As a direct result of AFR's violation of the New Jersey CFA, Plaintiffs and the Class are entitled to damages in an amount to be proven at trial as well as injunctive relief, including, but not limited to, ordering AFR to: (a) strengthen their data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) immediately provide adequate credit monitoring to all Class Members. Plaintiffs and Class Members were injured because they: (a) they would not have paid for Defendant's services had they known the true nature and character of AFR's data security practices; (b) would not have entrusted their PII to AFR in the absence of promises that Defendant would keep their information reasonably secure; and/or (c) would not have entrusted their PII to Defendant in the absence of the promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

274. On behalf of themselves and other members of the Class, Plaintiffs are entitled to recover legal and/or equitable relief, including an order enjoining AFR's unlawful conduct, treble damages, costs, and reasonable attorneys' fees pursuant to N.J.S.A. § 56:8-19, and any other just and appropriate relief.

CLAIM ON BEHALF OF THE ALTERNATIVE MARYLAND CLASS

COUNT VI

MARYLAND CONSUMER PROTECTION ACT

Md. Comm. L. Code § 13-301, et seq.

(On Behalf of Plaintiff Micah and the Alternative Maryland Class)

275. Plaintiff Micah repeats the allegations contained in paragraphs 1 through 193 as if fully set forth herein.

276. Plaintiff Micah brings this claim on behalf of herself and the alternative Maryland Class.

277. Plaintiff Micah and the Maryland Class are “consumers” under Md. Comm. L. Code § 13-101(c).

278. AFR is a “person” under Md. Comm. L. Code § 13-101(h) and offered, advertised, or sold “consumer services” as defined in Md. Comm. L. Code § 13-101(d).

279. AFR engaged in the acts and practices alleged herein in the state of Maryland with respect to Plaintiff Micah and the Maryland Class.

280. Recovery under the Maryland Consumer Protection Act (“MCPA”) may be had for unfair as well as deceptive conduct. *Legg v. Castruccio*, 642 A.2d 906, 913 (Md. Ct. Spec. App. 1994); *Hibdon v. Safeguard Props., LLC*, No. PJM 14-591, 2015 WL 4249525 at *4 (D. Md. July 9, 2015). In determining whether conduct is unfair under the MCPA, courts consider: (a) whether there was a substantial injury; (b) that is not outweighed by any countervailing benefits to the consumer or to competition that the practice produces; and (c) must not be the type of injury that a consumer could reasonably have avoided. *Id.*

281. Here, Defendant's conduct was unfair under the MCPA. First, AFR's failure to safeguard Plaintiff Micah's and the Maryland Class' PII and leaving it exposed to cyber criminals and unauthorized actors constitutes a substantial injury since they both suffered actual injury from Defendant's unfair practices and are further at a substantial and imminent risk of identity theft. AFR still possesses Plaintiff Micah's and the Maryland Class' PII, and that PII has been both accessed and misused by unauthorized third parties, which is evidence of a substantial and imminent risk of identity theft for Plaintiff Micah and the Maryland Class. Plaintiff Micah and the Maryland Class will have to spend the remainder of their lives at greater risk for identity theft and fraud (having to constantly monitor for the same).

282. Second, there is no countervailing benefit for failing to have adequate data security. Defendant failed to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act for safeguarding PII. In allowing the Data Breach to occur, Defendant failed to: (a) maintain adequate data security to keep Plaintiff Micah's and the Maryland Class' sensitive PII from being stolen by cybercriminals; (b) properly secure and protect Plaintiff Micah's and the Maryland Class' PII; (c) adequately train employees to protect Plaintiff Micah's and the Maryland Class' PII; (d) adequately monitor its own data security systems for existing or potential intrusions; (e) adequately encrypt Plaintiff Micah's and the Maryland Class' PII; and (f) take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff Micah's and the Maryland Class' PII and other personal information from further unauthorized disclosure, release, data breaches, and theft. Accordingly, AFR's inability to safeguard Plaintiff Micah's and the Maryland Class' PII offends public policy, including Maryland legislative policy under the Maryland Personal Information Protection Act, Md. Comm. L. Code § 14-3503.

283. Third, AFR's failure to safeguard Plaintiff Micah's and the Maryland Class' PII and leaving it exposed to cyber criminals and unauthorized actors constitutes a substantial injury that Plaintiff Micah and the Maryland Class could not have reasonably avoided because Plaintiff Micah and the Maryland Class had no choice but share their PII with AFR to receive services from AFR in order to obtain or service a mortgage.

284. Additionally, AFR violated FTC regulations by failing to: (a) promptly dispose of PII when no longer required to be stored; (b) encrypt information stored on its computer networks; (c) understand vulnerabilities of its network; (d) implement policies to correct security problems; (e) use an intrusion detection system to expose a breach as soon as it occurs; (f) monitor all incoming traffic on its network for activity indicating someone is attempting to hack the system; (g) watch for large amounts of data being transmitted from the system; and (h) have a response plan ready in the event of a breach. These failures constitute unfair acts or practices, subjecting them to liability under the MCPA.

285. Moreover, AFR engaged in acts or practices deemed "unfair" by the FTC under Section 5 of the FTC Act.

286. Maryland courts rely on FTC regulations and guidance in interpreting "unfairness" under the MCPA. *See Sullivan v. YES Energy Mgmt., Inc.*, No. GJH-22-0418, 2022 WL 4777791, at *9 (D. Md. Sept. 20, 2022) ("in the same way that Section 5 of the FTC Act bars 'unfair or deceptive acts or practices in or affecting commerce,' the MCPA likewise bars '[u]nfair, abusive, or deceptive trade practices,' including those plausibly alleged here") (internal citation omitted); *Hibdon*, 2015 WL 4249525 at *5-*6.

287. The FTC has repeatedly concluded, and the Third Circuit agreed, that a company that fails to have adequate data security in place commits an “unfair” trade practice in violation of Section 5 of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 246-47 (3d Cir. 2015) (holding that a company’s alleged failure to maintain reasonable and appropriate data security, if proven, could constitute an unfair method of competition in commerce under Section 5 of the FTC Act); *see also LabMD, Inc. v. FTC*, 894 F.3d 1221 (11th Cir. 2018) (affirming that the FTC’s prosecution of a company for inadequate data security measures with respect to health data is appropriate under Section 5’s “unfair” provision); *In re Brinker Data Incident Litig.*, No. 3:18-cv-686-J-32MCR, 2020 WL 691848, at *12 (M.D. Fla. Jan. 27, 2020) (“Because Plaintiffs allege that Brinker violated the FTC Act by providing inadequate security for customer data, they have alleged an unfair practice”); *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1327 (N.D. Ga. 2019) (“The failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information can constitute an unfair method of competition in commerce in violation of the [FTC] Act.”); Federal Trade Commission, *Cases Tagged with Privacy and Security*, <https://www.ftc.gov/enforcement/cases-proceedings/terms/1420> (collecting FTC enforcement cases).

288. As a result of AFR’s unfair acts and practices in violation of the MCPA, Plaintiff Micah and the Maryland Class have suffered and will continue to suffer injury, losses of money or property, and monetary and non-monetary damages as alleged more fully above.

289. Plaintiff Micah and the Maryland Class seek all relief allowed under law for these violations, including damages, disgorgement, injunctive relief, and attorneys’ fees and costs.

CLAIM ON BEHALF OF THE ALTERNATIVE ILLINOIS CLASS

COUNT VII

ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, 815

Ill. Comp. Stat. § 505/1, et seq.

(On Behalf of Plaintiff Stuart and the Alternative Illinois Class)

290. Plaintiff Stuart repeats the allegations contained in paragraphs 1 through 193 as if fully set forth herein.

291. Plaintiff Stuart brings this claim on behalf of himself and the alternative Illinois Class.

292. Plaintiff Stuart and the Illinois Class are “consumers” as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiff Stuart, the Illinois Class, and AFR are “persons” as defined in 815 Ill. Comp. Stat. § 505/1(c).

293. AFR is engaged in “trade” or “commerce,” including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). AFR engages in the sale of “merchandise” (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

294. The Illinois Consumer Fraud and Deceptive Business Practices Act (“ICFA”) is a “regulatory and remedial statute intended to protect consumers, borrowers, and business persons against fraud, unfair methods of competition, and other unfair and deceptive business practices.” *Robinson v. Toyota Motor Credit Corp.*, 775 N.E.2d 951, 960 (Ill. 2002), *Hill v. PS Ill. Tr.*, 856 N.E.2d 560, 568 (Ill. App. Ct. 2006). It is to be liberally construed to effectuate its purpose. *Robinson*, 775 N.E.2d at 960.

295. Recovery under ICFA may be had for unfair conduct, as well as deceptive conduct. *Robinson*, 775 N.E.2d at 960. In determining whether conduct is unfair under the ICFA, courts consider: (a) whether the practice offends public policy; (b) whether it is oppressive, immoral, unethical, or unscrupulous; and (c) whether it causes consumers substantial injury. *Boyd v. U.S. Bank, N.A.*, 787 F. Supp. 2d 747, 751 (N.D. Ill. 2011); *Duby v. Public Storage, Inc.*, 918 N.E.2d 265, 277 (Ill. App. Ct. 2009). A practice can be unfair without meeting all three criteria. *Id.*

296. Here, Defendant's conduct is unfair under the ICFA. First, Defendant failed to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act for safeguarding PII. In allowing the Data Breach to occur, Defendant failed to: (a) maintain adequate data security to keep Plaintiff Stuart's and the Illinois Class' sensitive PII from being stolen by cybercriminals; (b) properly secure and protect Plaintiff Stuart's and the Illinois Class' PII; (c) adequately train employees to protect Plaintiff Stuart's and the Illinois Class' PII; (d) adequately monitor its own data security systems for existing intrusions; (e) encrypt or adequately encrypt Plaintiff Stuart's and the Illinois Class' PII; (f) timely and adequately inform Plaintiff Stuart and the Illinois Class of the Data Breach; and (g) take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff Stuart's and the Illinois Class' PII and other personal information from further unauthorized disclosure, release, data breaches, and theft. Accordingly, AFR's inability to safeguard Plaintiff Stuart's and the Illinois Class' PII offends public policy.

297. Second, Defendant's conduct against Plaintiff Stuart and the Illinois Class is oppressive in that Plaintiff Stuart and the Illinois Class had no choice but share their PII with AFR in order to receive a mortgage. On information and belief, all mortgage companies require this information, so Plaintiff Stuart and Illinois Class members had no choice but to provide their PII to Defendant in order to receive a mortgage. Moreover, Plaintiff Stuart and the Illinois Class were assured by AFR that their PII would be secured, but once their PII was in AFR's possession, they had no ability on their own to protect the PII that was provided to AFR.

298. Third, AFR's failure to safeguard Plaintiff Stuart's and the Illinois Class' PII and leaving it exposed to cyber criminals and unauthorized actors constitutes a substantial injury since they are at a substantial and imminent risk of identity theft. AFR still possesses Plaintiff Stuart's and the Illinois Class' PII, and that PII has been both accessed and misused by unauthorized third parties, which is evidence of a substantial and imminent risk of identity theft for Plaintiff Stuart and the Illinois Class. Plaintiff Stuart and the Illinois Class will have to spend the remainder of their lives at greater risk for identity theft and fraud (having to constantly monitor for the same).

299. Additionally, AFR violated FTC guidelines by failing to: (a) promptly dispose of PII when no longer required to be stored; (b) encrypt information stored on computer networks; (c) understand vulnerabilities of its network; (d) implement policies to correct security problems; (e) use an intrusion detection system to expose a breach as soon as it occurs; (f) monitor all incoming traffic for activity indicating someone is attempting to hack the system; (g) watch for large amounts of data being transmitted from the system; and (h) have a response plan ready in the event of a breach. These failures constitute unfair acts or practices, subjecting them to an ICFA claim. 15 U.S.C. § 45.

300. In sum, AFR's numerous failures in safeguarding Plaintiff Stuart's and the Illinois Class' PII violates ICFA.

301. As a result, Plaintiff Stuart and the Illinois Class have suffered and will suffer substantial injury, including, but not limited to: (a) the compromise, publication, theft, and/or unauthorized use of their PII; (b) out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft and fraud; (c) lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and the future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; (d) the continued risk to the publication of their PII, which remains in the possession of AFR and is subject to further breaches so long as AFR fail to undertake appropriate measures to protect PII in their possession; and (e) current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff Stuart and the Illinois Class.

302. AFR's failure to safeguard Plaintiff Stuart's and Illinois Class' PII in violation of FTC guidelines was the direct and proximate cause of damages incurred by Plaintiff Stuart and the Illinois Class.

303. AFR's wrongful practices were and are injurious to the public because those practices were part of AFR's generalized course of conduct that applied to the Illinois Class. Plaintiff Stuart and the Illinois Class have been adversely affected by AFR's conduct and the public was and is at risk as a result thereof.

304. As a result of AFR's wrongful conduct, Plaintiff Stuart and the Illinois Class were substantially injured in that they never would have provided their PII to AFR, or paid for AFR's services, had they known or been told that AFR failed to maintain sufficient security to keep their PII from being hacked and taken and misused by others.

305. As a direct and proximate result of Defendants' violations of the ICFA, Plaintiff Stuart and the Illinois Class have suffered harm, including: (a) actual instances of identity theft; (b) loss of time and money resolving fraudulent charges; (c) loss of time and money obtaining protections against future identity theft; (d) financial losses related to the payments or services made to AFR or AFR's customers that Plaintiff Stuart and the Illinois Class would not have made had they known of AFR's inadequate data security; (e) lost control over the value of their PII; (f) unreimbursed losses relating to fraudulent charges; (g) harm resulting from damaged credit scores and information; and (h) other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

306. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff Stuart and the Illinois Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of AFR's violations of the ICFA.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

- A. For an Order certifying the Nationwide Class, or alternatively, the Florida, Maryland, Illinois, and Pennsylvania Classes, and appointing Plaintiffs and their counsel to represent the certified Class and/or Classes;
- B. For equitable relief enjoining AFR from engaging in the wrongful conduct complained of herein pertaining to the misuse, disclosure of, and/or failure to adequately secure Plaintiffs' and Class Members' PII;

- C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including, but not limited to, an Order:
- i. prohibiting AFR from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring AFR to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - iii. requiring AFR to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless AFR can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;
 - iv. requiring AFR to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' PII;
 - v. prohibiting AFR from maintaining Plaintiffs' and Class Members' PII on a cloud-based database;
 - vi. requiring AFR to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on AFR's systems on a periodic basis, and ordering AFR to promptly correct any problems or issues detected by such third-party security auditors;
 - vii. requiring AFR to engage independent third-party security auditors and internal personnel to run automated security monitoring;
 - viii. requiring AFR to audit, test, and train its security personnel regarding any new or modified procedures;
 - ix. requiring AFR to segment data by, among other things, creating firewalls and access controls so that if one area of AFR's network is compromised, hackers cannot gain access to other portions of AFR's systems;
 - x. requiring AFR to conduct regular database scanning and securing checks;
 - xi. requiring AFR to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting Plaintiffs' and Class Members' PII;

- xii. requiring AFR to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. requiring AFR to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with AFR's policies, programs, and systems for protecting PII;

- xiv. requiring AFR to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor AFR's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
 - xv. requiring AFR to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
 - xvi. requiring AFR to implement logging and monitoring programs sufficient to track traffic to and from AFR's servers; and
 - xvii. for a period of ten years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate AFR's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.
- D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;
- E. For an award of restitution for unjust enrichment;
- F. For an award of treble damages in accordance with the New Jersey CFA;
- G. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- H. For prejudgment interest on all amounts awarded; and
- H. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMAND

A jury trial is demanded by Plaintiffs and the putative Class Members as to all issues so triable.

DATED: April 28, 2023

**CARELLA, BYRNE, CECCHI, OLSTEIN,
BRODY & AGNELLO, P.C.**
JAMES E. CECCHI
LINDSEY H. TAYLOR

/s/ James E. Cecchi
JAMES E. CECCHI

5 Becker Farm Road
Roseland, NJ 07068
Telephone: 973/994-1700
Facsimile: 973/994-1744
jcecchi@carellabyrne.com
ltaylor@carellabyrne.com

**ROBBINS GELLER RUDMAN
& DOWD LLP**

STUART A. DAVIDSON
ALEXANDER C. COHEN
225 NE Mizner Boulevard, Suite 720
Boca Raton, FL 33432
Telephone: 561/750-3000
Facsimile: 561/750-3364
sdavidson@rgrdlaw.com
acohen@rgrdlaw.com

Plaintiffs' Co-Lead Interim Class Counsel

**MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC**

GARY M. KLINGER
227 West Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
gklinger@milberg.com

**MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC**

DAVID K. LIETZ
5335 Wisconsin Avenue NW, Suite 440
Washington, DC 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

THE LYON FIRM, LLC

JOSEPH M. LYON

2754 Erie Avenue

Cincinnati, OH 45208

Phone: (513) 381-2333

Fax: (513) 721-1178

jlyon@thelyonfirm.com

**MARKOVITS, STOCK
& DEMARCO, LLC**

TERENCE R. COATES

119 E. Court Street, Suite 530

Cincinnati, OH 45202

Phone: (513) 651-3700

Fax: (513) 665-0219

tcoates@msdlegal.com

**KANTROWITZ, GOLDHAMER &
GRAIFMAN, P.C.**

GARY S. GRAIFMAN

MELISSA R. EMERT

135 Chestnut Ridge Road, Suite 200

Montvale, NJ 07645

T: 845-356-2570

F: 845-356-4335

ggraifman@kgglaw.com

memert@kgglaw.com

Plaintiffs' Interim Class Counsel